

Separable extensions of orthogonal involutions in characteristic two

A.-H. Nokhodkar

Department of Pure Mathematics, Faculty of Science, University of Kashan,

P. O. Box 87317-51167, Kashan, Iran.

a.nokhodkar@kashanu.ac.ir

Abstract

It is shown that an anisotropic orthogonal involution in characteristic two is totally decomposable if it is totally decomposable over a separable extension of the ground field. In particular, this settles a characteristic two analogue of a conjecture formulated by Bayer-Fluckiger et al.

Mathematics Subject Classification: 16W10, 16K20, 11E04.

1 Introduction

The theory of involutions on central simple algebras is a generalization of the theory of symmetric bilinear forms. Given the fundamental role which Pfister forms play in the modern theory of bilinear forms, it is natural to ask whether there is a type of algebras with involution naturally generalising these forms. Since the adjoint involution of a Pfister form is totally decomposable, the class of totally decomposable involutions is a good candidate for this generalisation. Considering this fact and basic properties of Pfister forms, the following conjecture was formulated in [1]:

Conjecture 1.1. Let F be a field of characteristic not two and let (A, σ) be an algebra with orthogonal involution of degree 2^n over F . Then the following statements are equivalent:

- (1) (A, σ) is totally decomposable.
- (2) For every field extension K/F , $(A, \sigma)_K$ is either anisotropic or hyperbolic.
- (3) For every splitting field K of A , $(A, \sigma)_K$ is adjoint to a Pfister form.

The implications $(1) \Rightarrow (2)$, $(1) \Rightarrow (3)$ and $(2) \Leftrightarrow (3)$ are already known (see [2, Theorem 1], [7, (1.1)] and [4, (3.2)]). However, the implication $(2) \Rightarrow (1)$ or $(3) \Rightarrow (1)$ is still open in general, only known for algebras of low index or degree or in certain special cases.

An analogous conjecture in characteristic two was formulated in [6] with two differences: (i) it was assumed that σ is anisotropic; (ii) the hyperbolicity

condition in (2) was replaced by the metaboly. Note that the restriction to anisotropic involutions is reasonable as this restriction also must be made for the corresponding statement for bilinear Pfister forms in characteristic two (see [6, (5.5)]). The implications (1) \Rightarrow (2) and (2) \Rightarrow (3) were proved in [6]. Also, a proof of (3) \Rightarrow (1) is recently obtained in [12].

According to [6, (3.3)], a symmetric bilinear form over a field F of characteristic two is similar to a Pfister form if it is similar to a Pfister form over some separable extension of F . An analogue question for involutions may be considered as follows: let (A, σ) be a central simple algebra with involution over a field F of characteristic two. Given that $(A, \sigma)_K$ is totally decomposable for some separable extension K/F , does it imply that (A, σ) is totally decomposable? This question is in fact a generalization of the implication (3) \Rightarrow (1) of Conjecture 1.1 in characteristic two.

In this work, we study the above question for anisotropic orthogonal involutions. Our approach is based on a totally singular quadratic form q_σ associated to every orthogonal involution σ in characteristic two. This form was defined in [11] and used to obtain some sufficient conditions for anisotropy of orthogonal involutions. Although the form q_σ is not functorial, it will be shown in Theorem 3.5 that if K/F is a separable extension then $q_{\sigma_K} \simeq (q_\sigma)_K$. We then prove in Theorem 4.4 that an F -algebra with anisotropic orthogonal involution (A, σ) in characteristic two is totally decomposable if $(A, \sigma)_K$ is totally decomposable for some separable extension K/F (note that this result is already known to be false if σ is isotropic; see Remark 4.5). As an application, we prove in Theorem 4.6 that the three conditions of Conjecture 1.1 (in characteristic two) are equivalent to:

(4) $(A, \sigma)_K$ is totally decomposable for some separable extension K/F .

2 Preliminaries

In this work, all fields are implicitly supposed to be of characteristic two. Let V be a finite-dimensional vector space over a field F and let q be a quadratic form on V . We say that q is *isotropic* if $q(v) = 0$ for some nonzero vector $v \in V$ and *anisotropic* otherwise. The quadratic form q is called *totally singular* if there exists a symmetric bilinear form \mathfrak{b} on V such that $q(v) = \mathfrak{b}(v, v)$ for every $v \in V$. For a field extension K/F , the scalar extension of q to K is denoted by q_K .

Let A be a central simple algebra over a field F . An *involution* on A is an anti-automorphism of order two of A . If σ is an involution on A then the restriction $\sigma|_F$ is an automorphism which is either the identity map or of order two. If $\sigma|_F = \text{id}$ we say that σ is of *the first kind*. Otherwise, it is said to be of *the second kind*. An involution of the first kind on A is called *symplectic* if it becomes adjoint to an alternating bilinear form over a splitting field of A . Otherwise, it is called *orthogonal*. The sets of *symmetric* and *alternating* elements of an algebra with involution (A, σ) are defined respectively as

$$\text{Sym}(A, \sigma) = \{x \in A \mid \sigma(x) = x\} \quad \text{and} \quad \text{Alt}(A, \sigma) = \{x - \sigma(x) \mid x \in A\}.$$

According to [9, (2.6)], an involution σ of the first kind on A is orthogonal if and only if $\text{Alt}(A, \sigma) \cap F = \{0\}$. An involution σ on A is called *isotropic* if there exists a nonzero element $x \in A$ such that $\sigma(x)x = 0$ and *anisotropic* otherwise.

For a central simple algebra A over a field F the integer $\sqrt{\dim_F A}$ is called the *degree* of A and is denoted by $\deg_F A$. A central simple algebra of degree two is called a *quaternion algebra*. An algebra with involution is called *totally decomposable* if it decomposes as tensor products of quaternion algebras with involution.

3 Separable extensions of the alternator form

Let (A, σ) be a central simple algebra with orthogonal involution over a field F and set

$$S(A, \sigma) = \{x \in A \mid \sigma(x)x \in F \oplus \text{Alt}(A, \sigma)\}.$$

Define a map $q_\sigma : S(A, \sigma) \rightarrow F$ as follows: if $x \in S(A, \sigma)$ then there exists a unique element $\alpha \in F$ satisfying $\sigma(x)x + \alpha \in \text{Alt}(A, \sigma)$; set $q_\sigma(x) = \alpha$. By [11, (3.2) and (3.3)], the set $S(A, \sigma)$ is an F -subalgebra of A and q_σ is a totally singular quadratic form on $S(A, \sigma)$. As in [11], we call q_σ the *alternator form* of (A, σ) . It is easily verified that if K/F is a field extension then $S(A, \sigma) \otimes K \subseteq S(A_K, \sigma_K)$ (see the proof of [11, (3.6)]). However, the definition of q_σ is not functorial by [11, (3.18)]. In this section we show that if K/F is a separable extension then $q_{\sigma_K} \simeq (q_\sigma)_K$.

Lemma 3.1. *Let (A, σ) be a central simple algebra with orthogonal involution over a field F . If K/F is a separable quadratic extension, then $S(A_K, \sigma_K) = S(A, \sigma) \otimes K$.*

Proof. We only need to prove $S(A_K, \sigma_K) \subseteq S(A, \sigma) \otimes K$. Write $K = F(\eta)$ for some $\eta \in K$ with $\delta := \eta^2 + \eta \in F$. Then every $x \in S(A_K, \sigma_K)$ can be written as $x = u \otimes 1 + v \otimes \eta$, where $u, v \in A$. We have

$$\begin{aligned} \sigma_K(x)x &= (\sigma(u) \otimes 1 + \sigma(v) \otimes \eta)(u \otimes 1 + v \otimes \eta) \\ &= (\sigma(u)u + \delta\sigma(v)v) \otimes 1 + (\sigma(u)v + \sigma(v)u + \sigma(v)v) \otimes \eta. \end{aligned} \quad (1)$$

Write $q_{\sigma_K}(x) = a \otimes 1 + b \otimes \eta$ for some $a, b \in F$, so that $\sigma_K(x)x + a \otimes 1 + b \otimes \eta \in \text{Alt}(A_K, \sigma_K)$. Since $\text{Alt}(A_K, \sigma_K) = \text{Alt}(A, \sigma) \otimes K$, using (1) we get

$$\sigma(u)u + \delta\sigma(v)v + a \in \text{Alt}(A, \sigma), \quad (2)$$

$$\sigma(u)v + \sigma(v)u + \sigma(v)v + b \in \text{Alt}(A, \sigma). \quad (3)$$

As $\sigma(u)v + \sigma(v)u \in \text{Alt}(A, \sigma)$, (3) implies that $\sigma(v)v + b \in \text{Alt}(A, \sigma)$, i.e., $v \in S(A, \sigma)$ and $q_\sigma(v) = b$. Using (2) we get

$$\sigma(u)u + a + b\delta = (\sigma(u)u + \delta\sigma(v)v + a) + \delta(\sigma(v)v + b) \in \text{Alt}(A, \sigma).$$

Hence, $u \in S(A, \sigma)$ and $q_\sigma(u) = a + b\delta$. It follows that $x \in S(A, \sigma) \otimes K$, proving the result. \square

Lemma 3.2. *Let (A, σ) be a central simple algebra with involution over a field F and let $x = \sum_{i=1}^n x_i$, where $x_1, \dots, x_n \in A$. Then $\sigma(x)x + \sum_{i=1}^n \sigma(x_i)x_i \in \text{Alt}(A, \sigma)$.*

Proof. We have

$$\sigma(x)x = \sum_{i=1}^n \sigma(x_i) \cdot \sum_{i=1}^n x_i = \sum_{i=1}^n \sigma(x_i)x_i + \sum_{i \neq j} \sigma(x_i)x_j.$$

Hence,

$$\begin{aligned} \sigma(x)x + \sum_{i=1}^n \sigma(x_i)x_i &= \sum_{i \neq j} \sigma(x_i)x_j = \sum_{i < j} \sigma(x_i)x_j + \sum_{i < j} \sigma(x_j)x_i \\ &= \sum_{i < j} (\sigma(x_i)x_j - \sigma(\sigma(x_i)x_j)) \in \text{Alt}(A, \sigma). \quad \square \end{aligned}$$

Lemma 3.3. *Let (A, σ) be a central simple algebra with orthogonal involution over a field F . If K/F is a field extension of odd degree, then $S(A_K, \sigma_K) = S(A, \sigma) \otimes K$.*

Proof. As already observed, it is enough to show that $S(A_K, \sigma_K) \subseteq S(A, \sigma) \otimes K$. Write $K = F(\eta)$ for some $\eta \in K$ and let $[K : F] = 2n + 1$. Then the set $\{1, \eta, \eta^2, \dots, \eta^{2n}\}$ is a basis of K over F . Let $x \in S(A_K, \sigma_K)$ and set $\alpha = q_{\sigma_K}(x) \in K$. Write $x = \sum_{i=0}^{2n} x_i \otimes \eta^i$, where $x_i \in A$ for $i = 0, \dots, 2n$. Since $\sigma_K(x)x + \alpha \in \text{Alt}(A_K, \sigma_K)$, Lemma 3.2 implies that

$$\sum_{i=0}^{2n} \sigma_K(x_i \otimes \eta^i) \cdot (x_i \otimes \eta^i) + \alpha \in \text{Alt}(A_K, \sigma_K).$$

Hence,

$$\sum_{i=0}^{2n} \sigma(x_i)x_i \otimes \eta^{2i} + \alpha \in \text{Alt}(A_K, \sigma_K). \quad (4)$$

Since $[K : F]$ is odd, we have $F(\eta^2) = K$, hence the set $\{1, \eta^2, \eta^4, \dots, \eta^{4n}\}$ is a basis of K over F . Write $\alpha = \sum_{i=0}^{2n} \alpha_i \otimes \eta^{2i}$ for some $\alpha_i \in F$, $i = 0, \dots, 2n$. Then (4) implies that

$$\sum_{i=0}^{2n} (\sigma(x_i)x_i + \alpha_i) \otimes \eta^{2i} \in \text{Alt}(A_K, \sigma_K).$$

It follows that $\sigma(x_i)x_i + \alpha_i \in \text{Alt}(A, \sigma)$, i.e., $x_i \in S(A, \sigma)$ for every i . \square

Using Lemma 3.1, Lemma 3.3 and basic Galois theory, we have the following result.

Corollary 3.4. *Let (A, σ) be a central simple algebra with orthogonal involution over a field F . If K/F is a finite separable extension, then $S(A_K, \sigma_K) = S(A, \sigma) \otimes K$.*

Theorem 3.5. *Let (A, σ) be a central simple algebra with orthogonal involution over a field F . If K/F is a separable extension, then $S(A_K, \sigma_K) = S(A, \sigma) \otimes K$ and $(S(A_K, \sigma_K), q_{\sigma_K}) \simeq (S(A, \sigma), q_{\sigma})_K$.*

Proof. We already know that $S(A, \sigma) \otimes K \subseteq S(A_K, \sigma_K)$. Let $x \in S(A_K, \sigma_K)$ and set $\alpha = q_{\sigma_K}(x) \in K$. As K/F is separable, one can find a subfield L of K containing F with $[L : F] < \infty$ for which $x \in A_L$ and $\alpha \in L$. We have

$$\sigma_L(x)x + \alpha = \sigma_K(x)x + \alpha \in \text{Alt}(A_K, \sigma_K) \cap A_L = \text{Alt}(A_L, \sigma_L).$$

It follows that $x \in S(A_L, \sigma_L)$. By Corollary 3.4 we have $x \in S(A, \sigma) \otimes L \subseteq S(A, \sigma) \otimes K$. This proves that $S(A_K, \sigma_K) = S(A, \sigma) \otimes K$. On the other hand, it is easily seen that $q_{\sigma_K}|_{S(A, \sigma) \otimes K} = (q_{\sigma})_K$ (see the proof of [11, (3.6)]). Hence, $q_{\sigma_K} = (q_{\sigma})_K$, proving the result. \square

Definition 3.6. An algebra with involution (A, σ) (or the involution σ itself) is called *direct* if there is no nonzero element $x \in A$ satisfying $\sigma(x)x \in \text{Alt}(A, \sigma)$.

Direct involutions were introduced in [5]. Note that every direct involution is anisotropic. Also, by [5, (9.3)] every direct involution stays direct over a separable extension of the ground field. We present here an alternative proof of this fact. Recall that any anisotropic totally singular quadratic form remains anisotropic over a separable extension. This follows from the corresponding result for bilinear forms (see [8, (10.2.1)]).

Corollary 3.7. *Let K/F be a field extension of odd degree and let (A, σ) be a central simple algebra with orthogonal involution over F . Then σ is direct if and only if σ_K is direct.*

Proof. According to [11, (3.8)], σ is direct if and only if q_σ is anisotropic. The conclusion therefore follows from Theorem 3.5 and the above result on separable extensions. \square

4 The main result

In this section we study orthogonal Pfister involutions in characteristic two. We first recall a definition from [10].

Definition 4.1. A unitary algebra R over a field F is called a *totally singular conic F -algebra* if $x^2 \in F$ for every $x \in R$.

In [10], it was shown that a central simple algebra of degree 2^n with involution of the first kind is totally decomposable if and only if there exists a 2^n -dimensional totally singular conic F -algebra $\Phi \subseteq \text{Sym}(A, \sigma)$, which is generated as an F -algebra by n elements and satisfies $C_A(\Phi) = \Phi$, where $C_A(\Phi)$ is the centralizer of Φ in A (see [10, (4.6)]). According to [10, (5.10)], if σ is orthogonal then Φ is uniquely determined, up to isomorphism.

The next result gives another criterion for an anisotropic orthogonal involution to be totally decomposable.

Proposition 4.2. *Let (A, σ) be a central simple algebra of degree 2^n with anisotropic orthogonal involution over a field F . Then (A, σ) is totally decomposable if and only if $S(A, \sigma) \subseteq \text{Sym}(A, \sigma)$ and $\dim_F S(A, \sigma) = 2^n$.*

Proof. The ‘only if’ implication follows from [11, (4.1)]. Conversely, suppose that $S(A, \sigma) \subseteq \text{Sym}(A, \sigma)$ be 2^n -dimensional. By [11, (3.10)], σ is direct. Hence, [11, (3.7)] implies that $S(A, \sigma)$ is a field satisfying $x^2 \in F$ for every $x \in S(A, \sigma)$. In particular, $S(A, \sigma)$ is a totally singular conic F -algebra. Since $\dim_F S(A, \sigma) = 2^n = \deg_F A$, $S(A, \sigma)$ is a maximal subfield of A , hence $C_A(S(A, \sigma)) = S(A, \sigma)$. Finally, note that $S(A, \sigma)$ is generated as an F -algebra by n elements, because $S(A, \sigma)$ is a field. Thus, (A, σ) is totally decomposable by [10, (4.6)]. \square

Recall that an algebra with involution (A, σ) (or the involution σ itself) over a field F is called *metabolic* if there is an idempotent $e \in A$ with $\dim_F eA = \frac{1}{2} \dim_F A$ such that $\sigma(e)e = 0$ (see [3, §A.1]). In this case, we say that e is a *metabolic* idempotent with respect to σ .

We now recall some definitions from [5].

Definitions 4.3. Let (A, σ) be a central simple algebra with involution over a field F . An algebra with involution (B, τ) is called a *part* of (A, σ) if there exist a symmetric idempotent $e \in A$ and an F -algebra isomorphism $f : eAe \xrightarrow{\sim} B$ such that $f \circ \tau = \sigma \circ f$ (note that the F -algebra eAe is central simple with unit element e). In this case, we say that e *defines* (B, τ) . The part of (A, σ) defined by $1 - e$ is called a *counterpart* of (B, τ) in (A, σ) . A part (B, τ) of (A, σ) is called the *anisotropic part* of (A, σ) , if (B, τ) is anisotropic and any counterpart of (B, τ) in (A, σ) is metabolic. We denote the anisotropic part of (A, σ) by $(A, \sigma)_{\text{an}}$. Finally, the *direct part* of (A, σ) is a part (C, ρ) of $(A, \sigma)_{\text{an}}$ which is direct and any of its counterparts in $(A, \sigma)_{\text{an}}$ is symplectic.

Note that by [5, (4.5) and (7.5)] the anisotropic and direct parts of (A, σ) are uniquely determined, up to isomorphism.

Theorem 4.4. *Let K/F be a separable field extension and let (A, σ) be a central simple algebra of degree 2^n with anisotropic orthogonal involution over F . Then (A, σ) is totally decomposable if and only if $(A, \sigma)_K$ is totally decomposable.*

Proof. The ‘only if’ implication is evident. Conversely, suppose that $(A, \sigma)_K$ is totally decomposable. Since σ is anisotropic, [5, (7.7)] implies that σ has nontrivial direct part. By [5, (9.3)] the direct part of σ_K is also nontrivial. In particular, σ_K is not metabolic. It follows from [6, (6.2)] that σ_K is anisotropic. By Proposition 4.2 we have

$$S(A_K, \sigma_K) \subseteq \text{Sym}(A_K, \sigma_K) \quad \text{and} \quad \dim_K S(A_K, \sigma_K) = 2^n.$$

We also have $S(A_K, \sigma_K) = S(A, \sigma) \otimes K$ by Theorem 3.5, hence $\dim_F S(A, \sigma) = 2^n$. Finally, the equality $\text{Sym}(A_K, \sigma_K) = \text{Sym}(A, \sigma) \otimes K$ implies that $S(A, \sigma) \subseteq \text{Sym}(A, \sigma)$. Hence, (A, σ) is totally decomposable by Proposition 4.2. \square

Remark 4.5. Theorem 4.4 is not true for isotropic involutions. Indeed, as observed in [6, (9.4)], there exist a field F and an F -algebra with isotropic orthogonal involution (A, σ) which is not totally decomposable, but $(A, \sigma)_K$ is totally decomposable for any splitting field K of A . Hence, in this case, Theorem 4.4 is false for every separable splitting field K of A .

The following result gives an alternative proof of [12, (3.9)].

Theorem 4.6. *For an algebra with anisotropic orthogonal involution (A, σ) of degree 2^n over a field F the following statements are equivalent:*

- (1) (A, σ) is totally decomposable.
- (2) For every field extension K/F , $(A, \sigma)_K$ is either anisotropic or metabolic.
- (3) For every splitting field K of A , $(A, \sigma)_K$ is adjoint to a Pfister form.
- (4) $(A, \sigma)_K$ is totally decomposable for some separable extension K/F .

Proof. The implications (1) \Rightarrow (2) and (2) \Rightarrow (3) were proved in [6, (6.2)] and [6, (8.3)] respectively. The implication (3) \Rightarrow (4) follows by taking K to be a separable splitting field of A and (4) \Rightarrow (1) follows from Theorem 4.4. \square

References

- [1] E. Bayer-Fluckiger, R. Parimala, A. Quéguiner-Mathieu, Pfister involutions. *Proc. Indian Acad. Sci. Math. Sci.* **113** (2003), no. 4, 365–377.
- [2] K. J. Becher, A proof of the Pfister factor conjecture. *Invent. Math.* **173** (2008), no. 1, 1–6.
- [3] G. Berhuy, C. Frings, J.-P. Tignol, Galois cohomology of the classical groups over imperfect fields. *J. Pure Appl. Algebra* **211** (2007), no. 2, 307–341.
- [4] J. Black, A. Quéguiner-Mathieu, Involutions, odd degree extensions and generic splitting. *Enseign. Math.* **60** (2014), no. 3-4, 377–395.
- [5] A. Dolphin, Decomposition of algebras with involution in characteristic 2. *J. Pure Appl. Algebra* **217** (2013), no. 9, 1620–1633.
- [6] A. Dolphin, Orthogonal Pfister involutions in characteristic two. *J. Pure Appl. Algebra* **218** (2014), no. 10, 1900–1915.
- [7] N. Karpenko, Hyperbolicity of orthogonal involutions. With an appendix by Jean-Pierre Tignol. *Doc. Math.* 2010, Extra volume: Andrei A. Suslin sixtieth birthday, 371–392.
- [8] M. Knebusch, Grothendieck-und Witttringe von nichtausgearteten symmetrischen Bilinearformen. (German) *S.-B. Heidelberger Akad. Wiss. Math.-Natur. Kl.* (1969/70), 93–157.
- [9] M.-A. Knus, A. S. Merkurjev, M. Rost, J.-P. Tignol, *The book of involutions*. American Mathematical Society Colloquium Publications, 44. American Mathematical Society, Providence, RI, 1998.
- [10] M. G. Mahmoudi, A.-H. Nokhodkar, On totally decomposable algebras with involution in characteristic two. *J. Algebra* **451** (2016), 208–231.
- [11] A.-H. Nokhodkar, Orthogonal involutions and totally singular quadratic forms in characteristic two. *Manuscripta Math.* doi:10.1007/s00229-017-0922-y, (2017).
- [12] A.-H. Nokhodkar, Pfister involutions in characteristic two. *Bull. London Math. Soc.* doi:10.1112/blms.12048, (2017).